PRAKTIK TERBAIK PRIVASI GLOBAL

BSA adalah advokat utama untuk industri perangkat lunak global, yang terdepan dalam pengembangan inovasi mutakhir, termasuk komputasi awan, analitik data, dan kecerdasan buatan. Teknologi yang menggunakan perangkat lunak semakin mengandalkan data, dan dalam beberapa kasus, data pribadi, hingga fungsi. Akibatnya, perlindungan data pribadi adalah prioritas penting bagi anggota BSA, dan kami sadar bahwa itu merupakan bagian penting dalam membangun kepercayaan pelanggan. Untuk itu, BSA mempromosikan pendekatan terpusat pada pengguna untuk privasi yang menyediakan mekanisme untuk mengontrol data pribadi mereka kepada konsumen. BSA juga mendukung kerangka kerja perlindungan data, yang memastikan penggunaan data pribadi sesuai dengan harapan konsumen, selagi memungkinkan perusahaan untuk mengejar kepentingan bisnis yang sah.

Ketika negara-negara di seluruh dunia mempertimbangkan pengembangan kerangka kerja perlindungan data, banyak yang berusaha mengidentifikasi praktik terbaik global untuk pendekatan masalah ini. BSA mendukung penerapan praktik terbaik yang meningkatkan transparansi pengumpulan dan penggunaan data pribadi; membolehkan dan menghormati informasi pilihan dengan menyediakan tata kelola atas pengumpulan dan penggunaan data tersebut; memberikan kontrol atas data pribadi kepada konsumen; menyediakan keamanan yang kuat; dan mempromosikan penggunaan data untuk tujuan bisnis yang sah. **Kami menyoroti praktik terbaik yang dapat membantu mencapai tujuan ini, dan berfungsi sebagai panduan yang berguna untuk pengembangan dan modifikasi kerangka kerja perlindungan data di seluruh dunia.**

MASALAH	PRAKTIK TERBAIK
Lingkup Wilayah	Kerangka kerja perlindungan data harus mengatur perilaku yang memiliki hubungan cukup dekat dengan negara. Hukum harus berlaku jika: (1) memiliki target penduduk secara khusus; (2) data pribadi yang merupakan objek pemrosesan, dengan sengaja dikumpulkan dari subyek data di negara tersebut pada saat pengumpulan; dan (3) pengumpulan tersebut dilakukan oleh suatu lembaga yang didirikan di negara tersebut melalui aturan yang tetap sehingga menghasilkan tingkat aktivitas yang nyata dan efektif.
Definisi Data Pribadi	Ruang lingkup informasi yang termasuk dalam definisi data pribadi harus berupa informasi terkait dengan konsumen yang teridentifikasi atau dapat diidentifikasi. Konsumen yang dapat diidentifikasi adalah orang yang dapat diidentifikasi, secara langsung atau tidak langsung, dengan upaya yang wajar, mengacu pada pengidentifikasi seperti nama konsumen, nomor identifikasi, data lokasi, pengidentifikasi online, atau salah satu atau beberapa faktor khusus untuk fisik konsumen, fisiologis, atau identitas genetik konsumen tersebut. Cakupan ruang lingkup informasi harus terkait dengan data pribadi, yang jika salah ditangani akan memiliki dampak berarti terhadap privasi konsumen. Data yang tidak diidentifikasi melalui tindakan teknis dan organisasi yang kuat untuk mengurangi risiko identifikasi ulang secara wajar tidak boleh meliputi data di bawah kerangka kerja.

MASALAH	PRAKTIK TERBAIK
Bahaya	Kerangka perlindungan data harus menyesuaikan perlindungan terhadap risiko bahaya bagi konsumen. Bahaya yang dapat dikenali harus merefleksikan cedera fisik, efek kerugian kesehatan, kerugian finansial, atau pengungkapan data pribadi sensitif yang tidak diharapkan oleh konsumen dan menciptakan tingginya potensi terjadinya kerugian.
Transparansi	Pengontrol data harus memberikan keterangan yang jelas dan dapat diakses terkait praktik mereka untuk menangani data pribadi, termasuk kategori data pribadi yang dikumpulkan, jenis pihak ketiga yang berbagi data, dan keterangan proses yang dilakukan oleh pengontrol untuk meninjau, meminta perubahan ke, meminta salinan, atau menghapus data pribadi.
Spesifikasi Tujuan	Data pribadi harus relevan dengan tujuan data tersebut dikumpulkan dan diperoleh dengan cara yang sah. Pengontrol harus menginformasikan kepada konsumen terkait tujuan pengumpulan data pribadi mereka, dan harus menggunakan data tersebut dengan cara yang sesuai dengan penjelasan tersebut, konteks transaksi, atau harapan wajar dari konsumen, atau dengan cara yang sesuai dengan tujuan awal data dikumpulkan. Pengontrol harus memberlakukan sistem tata kelola yang berupaya memastikan bahwa data pribadi digunakan dan dibagikan dengan cara yang sesuai dengan pernyataan tujuan.
Kualitas Data	Data pribadi harus relevan dengan tujuan penggunaan, dan apabila diperlukan untuk tujuan tersebut, harus akurat, lengkap, dan terkini.
Landasan untuk Pemrosesan	Kerangka kerja perlindungan data harus mengenali dan membolehkan pemrosesan data untuk berbagai alasan yang sah, termasuk tujuan bisnis yang sah dan konsisten dengan konteks transaksi atau harapan konsumen. Tujuan valid lainnya, termasuk pemrosesan sehubungan dengan pelaksanaan kontrak; untuk kepentingan umum atau kepentingan vital konsumen; harus mematuhi kewajiban hukum; atau berdasarkan pada persetujuan konsumen. Kerangka kerja perlindungan data seharusnya tidak membatasi upaya keamanan cyber yang sah dari organisasi; pelaksanaan tindakan untuk mendeteksi atau mencegah penipuan atau pencurian identitas; kemampuan untuk melindungi informasi rahasia; atau pelaksanaan atau pembelaan klaim hukum.
Persetujuan	Pengontrol harus membolehkan konsumen untuk membuat pilihan berdasarkan informasi, dan bilamana praktis dan tepat, kemampuan untuk memilih tidak ikut serta dari pemrosesan data pribadi mereka. Dalam menetapkan apakah persetujuan sesuai, persetujuan harus diberikan pada waktu dan dengan cara yang relevan dengan konteks transaksi atau hubungan organisasi dengan konsumen.
Pemrosesan Data Pribadi yang Sensitif	Data tertentu, seperti informasi rekening keuangan atau kondisi kesehatan, dapat dianggap sangat sensitif. Jika pemrosesan data sensitif berimplikasi pada peningkatan risiko privasi, pengontrol harus membolehkan konsumen memberikan persetujuan yang jelas untuk pengumpulan data sensitif.

MASALAH	PRAKTIK TERBAIK
Kontrol Konsumen	Konsumen harus dapat meminta informasi tentang apakah organisasi memiliki data pribadi yang berkaitan dengan konsumen, dan sifat dari data tersebut. Konsumen harus dapat mengajukan keberatan atas keakuratan data tersebut, dan jika perlu mengoreksi atau menghapus data tersebut. Konsumen juga harus mendapatkan salinan data pribadi yang diberikan kepada organisasi atau dibuat oleh konsumen. Organisasi harus fleksibel dalam menentukan cara dan format yang tepat untuk memberikan informasi ini kepada konsumen. Pengontrol yang menentukan cara dan tujuan pemrosesan data pribadi, harus bertanggung jawab untuk menanggapi permintaan ini. Pengontrol dapat menolak permintaan tersebut apabila beban atau biaya untuk memenuhi permintaan tersebut tidak masuk akal atau tidak proporsional dengan risiko terhadap privasi konsumen; untuk mematuhi persyaratan hukum; untuk memastikan keamanan jaringan; untuk melindungi informasi komersial rahasia; untuk tujuan penelitian; atau untuk menghindari pelanggaran privasi, kebebasan berbicara, atau hak-hak lain dari konsumen lainnya. Pengontrol juga harus menerapkan prosedur verifikasi aman, untuk mengautentikasi konsumen yang mengajukan permintaan, untuk mengatasi risiko bahaya pengungkapan informasi yang tidak tepat.
Pemberitahuan Keamanan dan Pelanggaran	Pengontrol dan pemroses harus melakukan tindakan keamanan yang wajar dan tepat — terkait volume dan sensitivitas data, ukuran dan kompleksitas bisnis, dan biaya alat yang tersedia — yang dirancang untuk mencegah akses, penghancuran, penggunaan, modifikasi, dan pengungkapan tanpa izin terhadap data pribadi. Pengontrol data harus segera memberi tahu konsumen, setelah menemukan pelanggaran data pribadi yang melibatkan perolehan tidak sah atas data pribadi yang tidak terenkripsi atau tidak tersentuh, yang menimbulkan risiko materi pencurian identitas atau penipuan keuangan. Pelanggaran tersebut dapat dilaporkan kepada badan pengawas secara berkala, bersama dengan langkah-langkah keamanan yang dilakukan oleh organisasi sebagai bagian dari persyaratan akuntabilitas.
Persyaratan Akuntabilitas	Pengendali harus mengembangkan kebijakan dan prosedur yang menyediakan pengamanan yang diuraikan di sini, termasuk menunjuk orang untuk mengoordinasikan program yang menerapkan pengamanan ini, dan memberikan pelatihan dan manajemen karyawan; secara berkala mengawasi dan menilai pelaksanaan program-program tersebut; dan bila perlu menyesuaikan praktik untuk mengatasi masalah yang muncul. Sebagai bagian dari langkah-langkah ini, pengontrol dapat melakukan penilaian risiko secara berkala saat memproses data sensitif, dan di mana pengontrol mengidentifikasi risiko bahaya yang signifikan, mendokumentasikan penerapan pengamanan yang tepat. Pemerintah tidak boleh memaksakan persyaratan untuk laporan penilaian risiko atau berkonsultasi sebelumnya dengan badan pengawas, karena melakukan hal tersebut dapat menimbulkan beban administrasi yang tidak perlu, dan menunda pengiriman layanan bernilai tanpa manfaat yang sesuai dengan perlindungan privasi.

MASALAH	PRAKTIK TERBAIK
Transfer Data Lintas Batas	Kerangka kerja perlindungan data harus memungkinkan dan mendorong arus data global, yang mendukung ekonomi global. Organisasi yang memindahkan data secara global harus menerapkan prosedur untuk memastikan data yang dipindahkan ke luar negeri terus terlindungi. Jika ada perbedaan sistem perlindungan data, pemerintah harus membuat alat untuk menjembatani celah tersebut dengan cara yang melindungi privasi dan memfasilitasi pemindahan data global. Kerangka kerja perlindungan data harus melarang persyaratan pelokalan data baik untuk sektor publik dan swasta, yang dapat menggagalkan upaya untuk menerapkan langkah-langkah keamanan, menghambat inovasi bisnis, dan membatasi penyediaan layanan bagi konsumen.
Kewajiban Pengontrol dan Pemroses/ Alokasi Kewajiban	Pengontrol data yang menentukan cara dan tujuan pemrosesan data pribadi, harus memiliki tanggung jawab utama untuk memenuhi privasi hukum dan kewajiban keamanan. Pemroses data yang memproses data atas nama pengontrol, harus bertanggung jawab untuk mengikuti petunjuk pengontrol sesuai dengan perjanjian kontrak. Pengontrol dan pemroses harus fleksibel untuk menegosiasikan persyaratan kontrak mereka sendiri, tanpa kewajiban bahasa preskriptif yang disediakan oleh hukum.
Ganti Rugi dan Sanksi	Pembuat aturan pusat harus memiliki alat dan sumber daya yang dibutuhkan untuk memastikan penegakan yang efektif. Ganti rugi dan sanksi dan harus sebanding dengan kerusakan yang diakibatkan oleh pelanggaran undang-undang perlindungan data. Hukuman perdata tidak boleh ditetapkan secara sewenang-wenang atau berdasarkan faktor-faktor yang tidak memiliki hubungan substansial dengan konteks dasar timbulnya kerusakan tersebut. Hukuman pidana tidak proporsional untuk pelanggaran hukum perlindungan data.